International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2016, pp. 364-368
e-ISSN:2278-621X

VIRTUALIZATION TECHNOLOGY: WORK WITH MULTIPLE OPERATING SYSTEMS ON A SINGLE SYSTEM

Suman Antony Lasrado[1], Clifrn Colaco[2] and Kevin Milan Sequeira[3]

Abstract- Virtualization is a technology that allows us to run more than one operating system in parallel on a single computer. Virtualization finds its applications across a wide range of areas like securing platforms, kernel debugging, server consolidation, migration, etc. The aim of virtual systems is to achieve better resource utilization by providing a single integrated platform based on collection of different and independent resources. Virtualization at various levels allows us to improve system security, cost reduction, reliability, and flexibility. This paper explains the basics of virtualization and its cost reduction, classification, security concerns and also addresses its benefits.

Keywords –Watermarking, Haar Wavelet, DWT, PSNR

I. INTRODUCTION

Why are we familiar with the concept of multiple processes running on a single system and sharing the resources from a single computer. This achieved by operating system acting as a single point of contact interfacing with the hardware resources and control their access to hardware resources by many multiple processes. In today's world, information Technology (IT) industry's focus more on virtualization technology which has increased in the past few years. However, the concept has been introduced much longer.An Operating system (OS) directly interacts with hardware in normal non virtualized case. Suppose if we want to run multiple OSon a single computer, we need to have a layer between the OS and the actual hardware. The layer can be termed as abstraction layer. This hardware layer force the operating system to think that it is directly interacting with the hardware [1].

This layer help the user to enable to run more than one OS on a single system. In virtualization, there hardware layer which is known as virtual machine monitor (VMM) or hypervisor in between the OS and hardware. Through virtual machine monitor, we can install more than one OS and this hardware abstraction layer fools the OS thinking that it is running its own resources, but actually it creates an illusion and the resources are shared are same [2].

II. HISTORY

Virtualization was 1st developed by the IBM in 1960's, because it needs to partition one massive mainframe into many logical instances and to run on one hardware platform because the host.

[1] *AIMIT,St Aloysius College Mangalore, Karnataka, India*
[2] *St Aloysius College, AIMIT,Mangaluru, Karnataka, India*
[3] *St Aloysius College, AIMIT,Mangaluru, Karnataka, India*

This feature was fictional because the maintenance of enormous mainframe computers became terribly tedious. This improves the atmosphere potency and reduces the upkeep because it runs the multiple processes on every VM at constant time[1].
The two major advantages offered by any virtualization technology area unit.
Resource sharing: In traditional atmosphere all the resources area unit dedicated to this running programs, whereas in virtualized atmosphere VMs shares the physical resources of the underlying host like memory, hard disk, and processor and therefore the network adapters.
Isolation: Virtualization provides the isolation between VMs that area unit running on the one physical hardware platform. That the programs running on every VM area unit freelance of 1 another and can't see one another.

III. TYPES OF VIRTUALIZATION

A. PARA VIRTUALISATION:

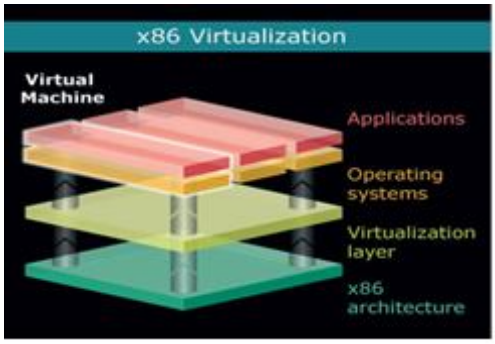
Here the virtualization provides Associate in nursing abstraction that is incredibly similar, however not fully just like the underlying hardware.VMware ESX andXen Virtual Machine server square measure samples of this method rather than fully emulating the underlying hardware design by the virtualization software package, the virtualized guests collaborate with the virtual machine or hypervisor to realize best performance. Para virtualization offers considerably improved performance; but, it needs modification to guest software. The guest OS is changed at low time to incorporate Para Virtualization extensions. Thence it needs cooperation from the OS merchant [3].
Eg: sun xVM virtual box

B. FULL VIRTUALIZATION

Here the virtualization software system provides a whole emulation of the underlying hardware. All software system may run on the underlying hardware can run as is, on the virtual machine. The software package doesn't want any modifications to be run as a guest OS instance. It can be any OS software package supported by the underlying hardware.
Eg: Virtual PC,VMware workstations, QEMU.

IV. HOW DOES VIRTUALIZATION WORK?

A virtual machine could be a tightly isolated package instrumentality which will run its own operative systems and applications as if it were a physical pc. A virtual machine behaves precisely sort of a physical pc and contains its own virtual (i.e., software-based) CPU, RAM, disk and network Interface card (NIC).
As software package can’t tell the distinction between a virtual machine and a physical machine, nor will applications or alternative computers on a network. Even the virtual machine thinks it's a real pc. Notwithstanding, a virtual machine consists entirely of package and contains no hardware parts any. As a result, virtual machines provide variety of distinct blessings over physical hardware.



The VMware virtualization platform is made on a business-ready design. Use package like VMware Infrastructure ANd VMware ESXi to remodel or virtualize the hardware resources of an x86 (32bit)based computer including the CPU, RAM, disk and network controller to produce a totally purposeful virtual machinehat will run its own software package and applications a bit like areal pc. VMware virtualization works by inserting a skinny layer of package directly on the pc hardware or on a bunch software package. This contains a hypervisor or virtual machine monitor that allocates hardware resources dynamically and transparently. Multiple operative systems run at the same time on one physical pc and share hardware resources with one another. By encapsulating a whole machine, as well as CPU, memory, software package, and network devices, a virtual machine is totally compatible with all commonplace x86 operative systems, applications, and device drivers. You'll be able to safely run many operative systems and applications at an equivalent time on one pc, with every having access to the resources it desires once it desires them [4].

V. VIRTUALIZATION BENEFITS

a. Load Balancing: As entire state of VM software system is totally captured by the VMM, it's comparatively straightforward to boost the performance via load leveling by migrating VMs to alternative platforms [5].

b. Virtual Hardware: Virtualization provides virtual hardware of the host like virtual LAN, virtual switches, memory area,virtual network adapters etc.

c. Flexibility: it's achieved in many ways. User will run quite one software system like applications in parallel on one system. It is attainable to maneuver the VMs to a different physical pc and has options like 'pause', 'resume', 'boot' and 'snapshot'. It additionally attainable to reconfigure the VMs whereas running, for example the scale of ram, network adapters, etc.

d. Availability: Even just in case of host cleanup for maintenance, VMs are often still ON by briefly migrating them to a different pc. By this fashion zero down time services area unit provided and might be terribly helpful whereas host hardware modification, upgrade and maintenance.

e. Hardware Utilization: This is often higher achieved once quite one VMs run on the host. VMs utilizes the idle resources that area unit left by the host OS

f. Security: it's achieved by the introduction of larger separation of services. Mutually VM is freelance of another VM, by running one service on every VM, even just in case if the service is affected the opposite VM services still remains unaffected. Every VM consists of a borderline OS install and one service. For example, the VM that hosts the digital computer that is file server

is affected; it does not affect the opposite running services just like the DNS server, DHCP server, information base server, etc [5].

g. Cost Reduction: It is done by combining smaller servers into single larger servers. In additionally achieved in terms of administration, floor area, software system licenses, and hardware.

h. Legacy Applications: throughout migration totally different OS, legacy applications area unit continued to run on recent OS, running as a guest with in VM. Therefore migration prices area unit reduced.

VI. SECURITY ISSUES IN VIRTUALIZATION

Most of the protection problems in virtualization atmosphere are same as within the physical system. The number of the issues that are common within the virtual atmosphere.

a. Communication between VMs or Between VMs and also the underlying Host.

One of the advantages of the virtualization is isolation that's VM applications are freelance of 1 another. If this profit isn't rigorously enforced then it'll be a significant cause to virtual atmosphere. Correct implementation of isolation ensures that the applications in one VM do not access different VM applications.

Strict maintenance of isolation ensures that forced the lock one VM do not give access either to different VM or underlying host. VMs and host system transfer information through a feature 'shared clipboard' within the VM. This feature could also be targeted by the malicious programs that may communicate between the VMs.

In a number of the VM technologies, the virtual machine layer is capable of work key strokes across the virtual terminals and hold on in host in order that host will monitor the logs of encrypted terminal connections within the virtual atmosphere . Some virtualization technologies do not implement isolation to support operation of OS specific applications on different OS resulting in exploitation of security carriers between in operation systems. So unlimited access to host resources gained creating it to vulnerable.

b. VM Escape.

VM shares the host resources and additionally provides the isolation between the VMs and host, and between VMs i.e., applications running in VM haven't got access to speak with either the opposite VM applications or host applications. Within the real atmosphere, organizations compromise on isolation so as to supply communication between the VMs, and between the host and VM therefore resulting in system security problems.

VM Escape is that the code bug caused by isolation compromise. Therefore programs running within the VM bypass the virtual layer or hypervisor layer, and gains host system privileges resulting in the exploit within the security framework of the system. It’s resolved by reconfiguring the interaction between the host and VM.

c. Denial of Service.

As the host system resources like memory, printer, electronic equipment ar shared by the VMs, there's an opportunity of inflicting the attack denial of service by one VM to different VMs running on an equivalent host. In virtual atmosphere this attack is caused once one VM holds all the resources of the underlying host. Therefore the host denies the opposite VMs request to resources. The most effective resolution to forestall this attack is to limit the resource access to every VM.

d. Monitoring VM from the Host.

In the virtual atmosphere, host is taken into account because the management purpose and there ar associations that the running VMs application is communicated with or monitored by the host. this suggests that the host should be secured instead of VMs. every virtualization technology has its own manner of host command to VM [2] just like the host will closing, reboot, suspend and resume the VMs, it may keep track of the offered resources to the VMs, and if given correct privileges then it may monitor the programs presently running within the VM. Additionally, it may monitor the VMs network traffic because it goes via the host, just in case if a bunch is attacked then it results in a security concern. Therefore, providing strict isolation avoids the prospect of assaultive VMs as host being the management purpose.

VII. CONCLUSION

Virtualization permits user to run over multiple operatingsystem in one system. It makes the work of an engineer terribly simple to judge his program at the same time in several software. It becomes simple for varied organizations to supply a replacement desktop for a newcomer with existing resources. Effective utilization of resources. So transfer and install a virtual box. Next install completely different operative systems of your wants and celebrate.

REFERENCES

[1] https://docs.oracle.com/cd/E27300_01/E27309/html/vmusg-virtualization.html
[2] http://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html
[3] https://www.virtualbox.org/wiki/Virtualization
[4] https://en.wikipedia.org/wiki/Virtualization
[5] http://www.vmware.com/solutions/virtualization.html